COT Security Alert – Phishing Emails Present Hazard to Email System and Data

Certain phishing emails arriving in state email inboxes are soliciting username and password information. A phishing email is an email which uses fraud in an attempt to acquire sensitive information such as usernames, passwords, bank information or credit card details by masquerading as a trustworthy entity, such as a bank, credit union or Information Technology department. **Phishing is a criminal activity.** Responding to phishing emails may help to finance criminal organizations or otherwise further promote nefarious activity.

When these emails are answered with state user logon credentials they give an unknown third party potential access to state government resources. Often this access allows the third party to send thousands of spam emails out to state users and the general public using state government email accounts and resources. This slows or ties up the state email system and uses a considerable amount of employee hours to stop the problem. In addition, the spam may cause *ky.gov* to be placed on underlined blacklists. Being blacklisted means that many legitimate state emails to destinations outside of the state network will not be allowed into their intended destination inboxes and associated state business cannot be conducted. In addition to the spam, personal information of Commonwealth citizens has the potential to be compromised.

As a reminder, there is ***never*** a time when a user's guard can go down. These emails constantly adapt to blocks and other methods of mitigation in order to land in more inboxes. Users are urged ***never*** to answer an email with personal information, including state logon credentials. This is never needed by COT or your agency's IT department. User's passwords should never be shared with anyone in accordance with Enterprise policy CIO-072 found on the COT website at http://technology.ky.gov/business/Pages/policies.aspx.

Distribution of this email to end-users may aid in awareness and reduce incidents of answered phishing emails.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/CISO/